(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 January 2003 (23.01.2003)

PCT

(10) International Publication Number
WO 03/007608 A1

(51) International Patent Classification[7]: H04N 7/167, H04L 9/06

(21) International Application Number: PCT/GB01/05232

(22) International Filing Date: 27 November 2001 (27.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0116713.9 9 July 2001 (09.07.2001) GB

(71) Applicant *(for all designated States except US)*: **AMINO HOLDINGS LIMITED** [GB/GB]; Longstanton House, Woodside, Longstanton, Cambridge (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **GILBERT, Martyn** [GB/GB]; 41 St. Michaels, Longstanton, Cambridge CB4 5BZ (GB).

(74) Agent: **REES, Alexander, Ellison**; Urquhart-Dykes & Lord, 30 Welbeck Street, London W1G 8ER (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 03/007608 A1

(54) Title: MOTION PICTURE ENCRYPTION METHOD AND APPARATUS WITH VARIABLE SECURITY

(57) Abstract: A method of variable security encryption, comprising the steps of: receiving a digital signal; selecting a variable number of data units from the digital signal; encrypting the selected data units; and replacing the selected data units with the corresponding encrypted data units; in which the number of data units selected can be varied. The resulting encrypted digital signal can be decrypted by reversing the encryption process.

MOTION PICTURE ENCRYPTION METHOD AND APPARATUS WITH VARIABLE SECURITY

This invention relates to a variable security encryption method for the encryption of digital data and apparatus for carrying out the method.

There is a general requirement to protect data against authorised review or copying and this requirement is particularly acute for digital data because of the great ease with which digital data can be copied and re-transmitted. Traditionally, such illicit review or copying of digital data has been prevented by encryption.

In general a method of encryption is selected having sufficient cryptographic strength that the resources required for an unauthorised third party to decrypt the digital data will be so great that the cost will exceed the value of the digital data or will take so long that the digital data has no value by the time it is decrypted. In selecting the encryption method account must also be taken of the resources required to carry out the encryption and for the legitimate intended recipient of the digital data to carry out decryption and any requirement to transmit additional data to support the encryption and decryption process over and above the digital data itself.

As a result, the selection of a suitable encryption method must take into account both the desired encryption strength and the cost in terms of the resources required to carry out the encryption and decryption and the amount of additional data which must be transmitted to support the encryption method.

This is a particular problem in the field of transmission of digital video signals. One reason is the very large amount of digital data making up a digital video signal, and where the digital video signal is being transmitted to subscribers for viewing the very high rate at which the digital data must be transmitted. A further reason is that when digital video signals are sent to subscribers to be viewed the equipment required to decrypt the digital video signal must be provided to each subscriber, for example as a set top box. As a result, in the encryption of digital video signals, increases in the resources required to encrypt and decrypt the signal cause particular difficulty because of the increase in the cost of the decryption equipment, such as a set top box provided to each subscriber. Further, because of the very large amount of digital video data to be transmitted in a digital video signal the increase in the

bandwidth required to send the digital signal including the additional data that must be sent to support the encryption and decryption process is particularly significant.

A further problem in applying conventional encryption methods to digital video signals is that where a digital video service is provided the value of different programming provided by the digital video varies from programme to programme. For example the economic value, that is the re-sale value of illicit copies of the program contents, of newly released films is much higher then the value of much of the rest of the programme contents, and the economic value of some programmes such as news reports or weather forecasts is very low and in some circumstances almost zero.

Accordingly, in view of the very different economic values of the programme contents for different programmes it would be desirable to encrypt them with different levels of cryptographic strength to reflect their different values. Using conventional methods of encryption this can only be done by using different encryption methods for different programs. However, this approach has the disadvantage of increasing the resources required by the equipment used to decrypt the signal because this must support several different encryption methods.

This invention was made in order to solve these problems, at least in part.

In a first aspect, this invention provides a method of variable security encryption, comprising the steps of:

receiving a digital signal;

selecting a variable number of data units from the digital signal;

encrypting the selected data units; and

replacing the selected data units with the corresponding encrypted data units;

in which the number of data units selected can be varied.

In a second aspect, this invention provides a method of encryption, comprising the steps of:

receiving a digital signal;

selecting a number of data units from the digital signal, such that the selected data units include only a part of the digital signal;

encrypting the selected data units; and

replacing the selected data units with the corresponding encrypted data units.

In a third aspect this invention provides a method of decryption comprising the steps of:

receiving a digital signal including a number of encrypted data units together with unencrypted data;

selecting the encrypted data units from the digital signal;

decrypting the selected data units; and

replacing the selected data units with corresponding decrypted data units.

In a fourth aspect, this invention provides variable security encryption apparatus comprising:

receiving means for receiving a digital signal;

selecting means for selecting a variable number of data units from the digital signal;

encryption means for encrypting the selected data units; and

means for replacing the selected data units with the corresponding encrypted data units;

in which the number of data units selected can be varied.

In a fifth aspect, this invention provides encryption apparatus comprising:

receiving means for receiving a digital signal;

selecting means for selecting a number of data units from the digital signal, such that the selected data units include only a part of the digital signal;

encryption means for encrypting the selected data units; and

means for replacing the selected data units with the corresponding encrypted data units.

In a sixth aspect, this invention provides decryption apparatus comprising:

receiving means for receiving a digital signal including a number of encrypted data units together with unencrypted data;

selection means for selecting the encrypted data units from the digital signal.

decrypting means for decrypting the selected data units; and

selection means for replacing the selected data units with corresponding decrypted data units.

This invention is based upon the realisation that in many types of digital data, and particularly in compressed video image data, there is a very low volume of redundant

information in the data. As a result, when protecting such data, even encrypting only a small percentage of the data is sufficient to render all of the data useless to anyone who is unable to decript the encrypted parts of the data.

Preferred embodiments of the invention will now be described, by way of example only, with reference to the accompanying diagrammatic figures, in which:

Figure 1 shows an encryption device according to the invention; and

Figure 2 shows a decryption device according to the invention.

A first embodiment of the invention is shown in Figure 1. Figure 1 shows in diagrammatic form an encryption device 1 according to the invention for encrypting a digital video signal to be transmitted as part of a pay per view or subscription digital video service. The encryption device 1 is supplied with an unencrypted digital video signal 2 made up of unencrypted digital data and produces an at least partially encrypted digital video signal 3. The encrypted digital video signal 3 is transmitted to authorised customers who are provided with the necessary decryption equipment to decrypt the encrypted digital video signal to reproduce the original unencrypted digital video signal for display on their equipment. Generally, the customers decryption equipment will be provided as a set top box or similar device.

The encryption device 1 comprises a slicer 4, an encryption engine 5 and a memory 6.

The slicer 4 receives the digital video signal 2 and divides it into blocks of a predetermined length. Each of the blocks of digital data comprises a number of units, in this example data bytes, of digital data. The slicer 4 operates on each of the blocks of digital data in turn to select some only of the data bytes making up the block of digital data.

The selected data bytes only are sent by the slicer 4 to the encryption engine 5 while the remaining, unselected, data bytes making up the block of digital data are sent to a holding memory 6 without being encrypted.

The encryption engine 5 individually encrypts the selected data bytes sent to it from the slicer 4 using an encryption method such that each encrypted byte has the same number of bits as the original unencrypted data byte.

The selected data bytes encrypted by the encryption engine 5 are then sent out by the encryption engine 5 and added to the remaining unencrypted data bytes of the block of digital data held in the memory 6 to form a block of encrypted digital video data having the same length as the original block of digital video data with the encrypted data bytes in the same positions in the block as the selected data bytes. The encrypted digital data block is then fed out of the memory 6 so that the series of encrypted digital data blocks are transmitted to the customer as an encrypted digital video signal.

The terms encrypted digital video signal and encrypted data block are used in this description although only a part of the digital data in the encrypted digital video signal and encrypted data block has been encrypted.

When the encrypted digital video signal is received by the customer, a customer decryption device decrypts the encrypted digital video signal to provide the original unencrypted digital video signal for display.

A decryption device 7 according to the invention is shown in Figure 2. The decryption device 7 comprises a slicer 4, a decryption engine 8 and a memory 9.

The decryption device 7 receives the encrypted digital video signal 3 and this is passed to a slicer 4. Similarly to the encryption device 1, the slicer 4 of the decryption device 7 divides the received digital video signal into a series of blocks of digital data having the same preset length as used by the slicer 4 of the encryption device 1 and each comprising a number of digital data bytes.

The slicer 4 selects the encrypted data bytes from each block of digital data and passes the encrypted data bytes to the decryption engine 8 for decryption. The remaining unselected digital data bytes of each block of digital data are stored in a memory 9.

The decryption engine 8 individually decrypts the selected received digital data bytes. The decrypted digital data bytes are then output from the decryption engine 8 and combined with the unselected digital data bytes in the memory 9 to reproduce the original digital data block and the digital data blocks are output sequentially by the decryption device 7 to provide the original video signal 2 for viewing by the customer.

The proportion of the data bytes in each block of digital data which are encrypted can be varied to change to the level of security to the level required by the content of the digital video signal. This proportion is called the slicer ratio.

The invention is not limited to the use of any particular encryption method by the encryption engine 5. However, whatever method of encryption is used by the encryption engine 5 the strength of the encryption of the total video signal as a whole, that is the time and resources required by an unauthorised third parties to decrypt it, will be greater if a larger number of data bytes are encrypted from each block of digital data.

This allows the amount of additional data which must be transmitted in order to carry out the encryption and decryption process, which additional data will increase the bandwidth required to transmit the digital video signal, to be reduced for programme content requiring a lower level of security and increased for programme content requiring a higher level of security with only a single decryption engine 8 being required by each customer decryption device 7.

The invention is particularly effective to protect a compressed digital video signal. This is because such a compressed signal has very little redundant information, so that the encrypted parts of the signal cannot be replaced. Further, many compression techniques employ delta compression mechanisms so that each bit has significance over a period of time. As a result, each bit which is encrypted and so cannot be recovered can interfere with the correct interpretation of a number of video and audio data blocks.

The proportional of the digital data which is encrypted, that is the proportion of the digital data bytes which are encrypted in each block of digital data, can be varied from 0 to 100%. In practice for digital video signals compressed using MPEG it has been found that encrypting only 3% of the digital video signal so that 3% of the digital data bytes in each block of digital data are encrypted is sufficient to prevent the digital video signal being identified as a digital video signal or displayed by conventional digital video decoding equipment such as that normally fitted in digital television set top boxes. Accordingly, this level of encryption is sufficient to prevent casual viewing of the encrypted digital video signal by unauthorised persons using conventional hardware. More determined cryptographic attacks could be made, for example by pirates wishing to make and distribute illicit copies of a film not yet on general release by recording the entire encrypted digital video signal and attempting to identify and decrypt the encrypted parts of the digital video signal.

However, the total amount of data in a digital video signal is very large and it is necessary to decrypt a very high proportion of the digital signal in order to produce a copy of

sufficient quality to have any economic value. As a result, attempted decryption using commonly available computing resources such as a conventional PC will not be able to decrypt the encrypted digital video signal in any useful period of time.

The example given above is for an MPEG compressed digital video signal. However, the invention is applicable to signals compressed using other compression protocols and to uncompressed signals.

The slicer 4 can operate by using a pseudo random number generator to select a number of data bytes from each block of digital data. Provided the slicers 4 in the encryption device 1 and the decryption device 7 have the same pseudo random algorithm, and the pseudo random number generators in both slicers 4 are seeded with the same value they can both select the same bytes for encryption and decryption. It is necessary for the slicers 4 in the encryption device 1 and decryption device 7 to be provided with a common pseudo random number generator seed and can this can be transmitted or supplied to the decryption device 7 by any suitable encryption key distribution system. It should be noted there is no requirement for data identifying the encrypted bytes within the encrypted digital video signal to be sent together with the digital video signal. As a result, there is no possibility of identifying the encrypted data bytes by analysis of the digital video signal and the amount of additional data which must be sent with the encrypted digital signal and the increase in bandwidth caused by encryption is minimised.

It is preferred that each of the blocks of digital video data in turn be held in the slicer 4 of the encryption device 1 while the selected data bytes to be sent to the encryption engine 5 are selected based on the numbers produced by the pseudo random number generator. This increases the flexibility of the system because this allows the bytes to be identified and selected in any order and not necessarily in a sequential order. For instance, in a system where the original data block was 20 data bytes in length and 2, that is, 10%, of the data bytes are to be selected for encryption the random number generator might instruct the slicer to first select the 17th data byte in the block followed by the 8th byte.

In some commercial applications it will be preferred for the seed value used in the pseudo random number generator in the slicers 4 of the encryption device 1 and the decryption device 7 to be the same each time the same digital data is encrypted. For example where the invention is used in a video on demand service where a digital video film is

encrypted and sent to each client individually it is important the same bytes of each block of digital data, that is the same bytes of the digital video signal are encrypted each time the encrypted film is sent. Otherwise a determined pirate could record the encrypted digital video signal a number of times and reassemble the original digital video signal from it by piecing together different parts of different copies to replace the encrypted data bytes of one copy with unencrypted data bytes from another copy. Such a process of substitution will be much simpler than the task of identifying and decrypting the encrypted data bytes in a single copy of the encrypted digital video signal.

Such a video on demand service could separately encrypt the digital video signal each time it is requested using the same starting seed for the pseudo random number generator. Alternatively the digital video signal could be encrypted once and recorded. The recorded encrypted digital video signal can then be sent each time a request to see the film is received.

In an alternative arrangement the pseudo random number generator used to select the bytes to be encrypted in the slicer 4 is replaced by a slicer array. This is an array having a number of entries equal to the number of bytes in each digital data block, with each entry being a number corresponding to a specific byte in the digital data block. Where a number of bytes are to be selected from each block, this number of entries from the slicer array are used to select the bytes.

Preferably, each digital data block is sliced based upon successive entries in the slicer array so that each digital data block has different bytes selected for encryption.

Where multiple copies of the same digital video signal are encrypted and sent out it is preferred for the same slicer array to be used each time for the reason explained above for the pseud random number generator of preventing the peicing together of the original signal from parts of different encrypted signals.

A preferred form of encryption engine 5 is a rotor encryption device which substitutes for each digital data byte to be encrypted a replacement data byte having the same number of bits.

The rotor can be formed by a look up table containing a number of unique entries equal to the number of possible byte values and an offset value. When a data byte for encryption is received the value of the data byte is added to the offset and the result used as a

look value used as an index into the look up table. The value identified from the table by this index look up value is used as the encrypted data value and is recorded as the new offset value for use with the next byte to be encrypted. Thus, the encrypted byte value is usually, but not always, different from the original byte value and the value of the original byte cannot be deduced from the encrypted byte value unless the rotor table values and offset are known.

For example, where the slicer selects a number of 8 bit data bytes from each block of digital data the rotor table will contain 256 unique entries corresponding to all 256 possible values of an 8 bit data byte together with an 8 bit data byte offset value. For instance, if a data byte having a value of 44 is received, this is encrypted by adding the value 44 to the offset value. If, for instance the offset value were 12, this would give a look up value of 56 to be used as an index to select one of the unique entries from the table. In this case the 56 entry in the table is 102 so the encrypted value of the data byte is given as 102 and the offset value to be used for the next data byte to be encrypted is set to 102.

The process is reversed to decrypt the data byte.

The encryption engine 5 can be formed by a number of rotors arranged in series with the encrypted data byte output by each rotor stage of the encryption engine 5 being used as an input data byte for the next rotor stage. That is, each rotor stage treats the output of the previous rotor stage as an unencrypted input. Where multiple rotor stages are used, the rotors should have independently randomly selected tables. As a result the tables of different rotor stages will usually be different but may sometimes be the same.

Typically each of the rotor stages will be started using a different offset value, but this is not essential.

The encryption by a rotor or rotors in the encryption engine 5 can be reversed by decryption using the same number of rotors in the decryption engine 8.

In the preferred embodiment where the encryption engine 5 is formed by rotors, the pseudo random number generator or slicer array used to select the data bytes to be encrypted from each block of digital data in the slicer 4 must be constrained so that no data byte is selected and encrypted twice within one block of digital data.

In the preferred embodiment, in order to allow the decryption of the encrypted digital video signal the decryption device 7 must be supplied with the seed value used for the pseudo

random number generator in the slicer 4 and also with the rotor table and rotor offset for each of the rotors used in the encryption and decryption engines 5 and 8.

These "keys" must be transferred securely to or be known in advance by the decryption device 7.

In a preferred embodiment, each block of digital data contains 256 bytes.

The present invention is effective to provide a system allowing encryption and decryption of large amounts of data at a high rate, such as digital video image data, because the simplicity and speed of the rotor encryption system allows data to be encrypted or decrypted at a high rate using relative modest equipment.

The invention can be carried out as a pipeline process in software or hardware to allow rapid encryption and decryption of large data volumes using relatively inexpensive equipment.

In order to increase the level of cryptographic security provided by the invention it is necessary to change the keys referred to above at regular intervals. A rotor table is a relatively large item of data whereas the rotor offset and slicer seed values are relatively small items of data. Accordingly, in most applications it will be preferred to change the rotor offsets and slicer seeds more frequently than the rotor tables. Where a plurality of rotors are used their rotor tables and offsets may be changed individually or all together as appropriate.

The encryption method of the preferred embodiment employs a pseudo random number generator and rotor offsets which change each time a data byte is selected and encrypted. If the transmission links between transmitter and receiver are imperfect so that some of the transmitted data is lost the pseudo random generator and rotor offsets in the encryption device 1 and decryption device 7 may not agree for the same byte, preventing decryption of the encrypted byte and thus the encrypted video data signal. In order to avoid this problem, the offsets and pseudo random number generator seed can be reset to pre-arranged values before each new data packet or section of the digital video signal, so that only a small amount of data is lost.

For example, when the digital video signal is an MPEG signal this resetting can be carried out before each MPEG I-frame.

In the description above the selection of data bytes from blocks of digital data is described. It is convenient to use data bytes but any other size of data unit could be selected

from a digital data blocks if preferred. In general, the larger the bit size of the data unit selected the greater the cryptographic strength of the encryption and the greater the amount of processing required to carry out the encryption and decryption operations.

The size of the rotor table depends on the number of bits in each data unit, for example if 11 bit data units are used each rotor table will contain 2,048 entries.

It is preferred that the size of the blocks of digital data and the selected data unit be such that each digital data block contains an integer number of data units. This is not essential but it makes the invention simpler to carry out in practice.

The level of cryptographic security provided by the invention can be varied by altering the slicer ratio, that is, the proportion of the digital signal data selected by the slicer for encryption.

Enhanced security can also be offered in the preferred embodiment described by changing the length of the data blocks and data units into which the unencrypted digital data signal is divided. Further, the number of rotors used to carry out the rotor encryption can be altered. Further, the life span of the rotor tables, offsets and pseudo random number generator seed, that is, the frequency with which they are replaced, can be changed.

Each of these characteristics can be changed in accordance with the security requirements of the digital data signal being transmitted and the need to perform processor load balancing so that the processing capacity of the encryption and decryption devices is not exceeded.

In this description the preferred embodiment of the invention has been described in terms of an unencrypted digital video signal being encrypted and transmitted and then being received and decrypted for display. The encryption method and apparatus of the invention is equally applicable to uses where the encrypted digital signal is stored or recorded in encrypted form or where an encrypted digital video signal is provided from a memory or recording device for decryption and display.

The described embodiments are examples only and other arrangements to carry the invention are possible. In particular, the illustrated examples are intended to show the functional interelationships of the parts only and are not intending to be limiting as to the actual physical arrangement of apparatus for carrying out the invention.

Alternative arrangements are possible, for example the data bytes output from the encryption engine 5 or decryption engine 8 could be output directly interleaved with bytes from the respective memory as the output from the encrypting or decrypting device instead of being reintegrated with the unselected data bytes within the respective memory 6 and 9. As another alternative, each block of digital data could be retained within the slicer 4 or an internal memory thereof while one data unit at a time was selected from the block of digital data, encrypted or decrypted and then replaced in the digital data block before the next data unit, if any, was selected.

The invention is particularly useful for the encryption and decryption of digital video signals and the described embodiments are discussed in terms of this application. However, it is believed that the invention is applicable to the protection of other forms of digital data.

In this description the digital video signal provided to the encryption device 1 and output from the decryption device 7 is described as an unencrypted digital video signal. This means only that these signals have not been encrypted by the method of the invention. These signals may be encrypted by some other means and accordingly the "decrypted" output signal from the decryption device 7 may require further decryption before it can be viewed.

The described preferred embodiments are regarded as being particularly advantageous for carrying out the invention but the person skilled in the art of digital processing will be able to envisage many other arrangements by which the described processing could be carried out within the scope of the invention.

Claims

1. A method of variable security encryption, comprising the steps of:
receiving a digital signal;
selecting a variable number of data units from the digital signal;
encrypting the selected data units; and
replacing the selected data units with the corresponding encrypted data units;
in which the number of data units selected can be varied.

2. A method of encryption according to claim 1, in which a pseudo-random algorithm is used to select the data units.

3. A method of encryption according to claim 1, in which a look up table is used to select the data units.

4. A method according to any preceding claim, in which the selected data units include only a part of the digital signal.

5. A method according to claim 4, in which the selected data units include at least 3% of the digital signal.

6. A method according to any preceding claim, in which the digital signal is a digital video signal.

7. A method according to any preceding claim, in which the received data signal is divided into a series of blocks of digital data and a variable number of data units are selected from each block.

8. A method according to any preceding claim in which the length of each block of digital data is an integer multiple of the length of a data unit.

9. A method according to any preceding claim in which each data unit is one byte.

10. A method according to any preceding claim in which the selected data units are encrypted using at least one look up table by, the value of the data unit being combined with an offset value to produce a look up value, the look up value being used as an index to the look up table, and the value identified in the look up table by the look up value being used as the encrypted data unit and as an offset value for encrypting the next data unit.

11. A method of encryption, comprising the steps of:
receiving a digital signal;
selecting a number of data units from the digital signal, such that the selected data units include only a part of the digital signal;
encrypting the selected data units; and
replacing the selected data units with the corresponding encrypted data units.

12. A method of decryption comprising the steps of:
receiving a digital signal including a number of encrypted data units together with unencrypted data;
selecting the encrypted data units from the digital signal;
decrypting the selected data units; and
replacing the selected data units with corresponding decrypted data units.

13. Variable security encryption apparatus comprising:
receiving means for receiving a digital signal;
selecting means for selecting a variable number of data units from the digital signal;
encryption means for encrypting the selected data units; and
means for replacing the selected data units with the corresponding encrypted data units;
in which the number of data units selected can be varied.

14. Encryption apparatus comprising:

receiving means for receiving a digital signal;

selecting means for selecting a number of data units from the digital signal, such that the selected data units include only a part of the digital signal;

encryption means for encrypting the selected data units; and

means for replacing the selected data units with the corresponding encrypted data units.

15. Decryption apparatus comprising:

receiving means for receiving a digital signal including a number of encrypted data units together with unencrypted data;

selection means for selecting the encrypted data units from the digital signal.

decrypting means for decrypting the selected data units; and

selection means for replacing the selected data units with corresponding decrypted data units.

16. Encryption apparatus substantially as shown in or as described with reference to Figure 1 of the accompanying drawings.

17. Decryption apparatus substantially as shown in or as described with reference to Figure 2 of the accompanying drawings.

FIG.1

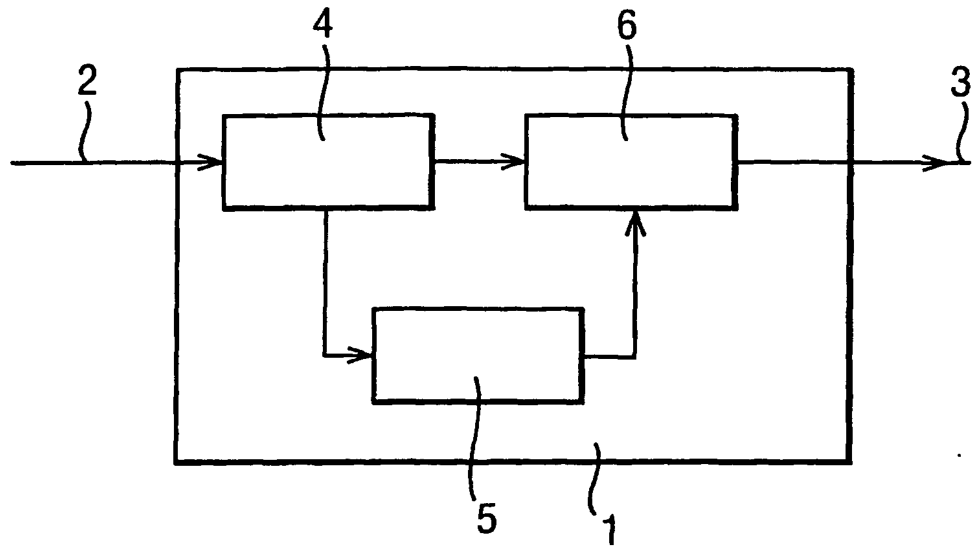
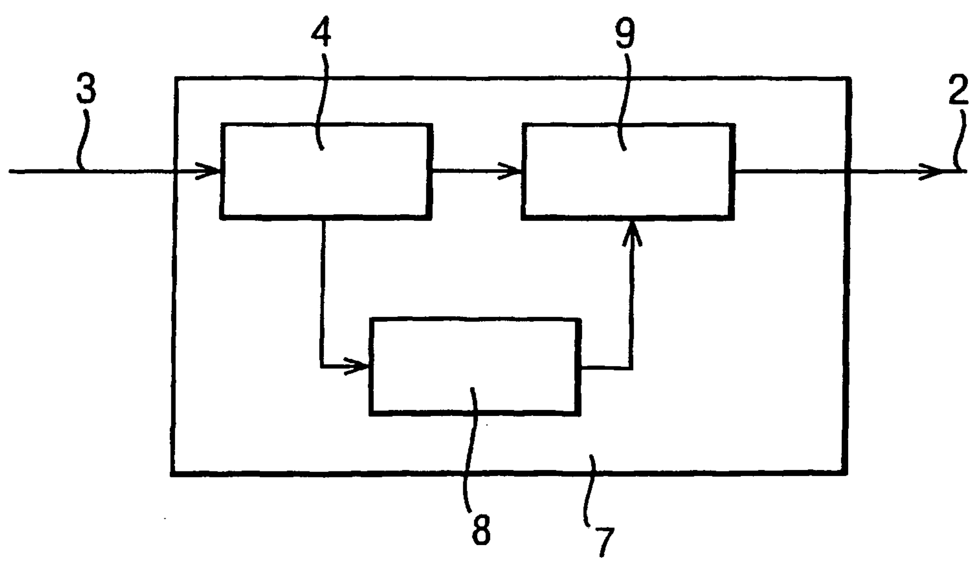


FIG.2



INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 01/05232

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 805 700 A (SHIPPY KEITH L ET AL) 8 September 1998 (1998-09-08) abstract column 1, line 1 - line 59	1,4,6,7, 11-15
Y	column 3, line 44 -column 4, line 41 figure 4	10
X	WO 00 60846 A (DIVA SYSTEMS CORP) 12 October 2000 (2000-10-12) page 3, line 1 - line 16	1,4,6,7, 11-15
A	page 24, line 4 -page 25, line 12	10

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 July 2002	07/08/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Liebhardt, I

Form PCT/ISA/210 (second sheet) (July 1992)

International Application No
PCT/GB 01/05232

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 021 199 A (ISHIBASHI YASUHIRO) 1 February 2000 (2000-02-01) column 2, line 14 - line 50 column 4, line 4 - line 32 column 5, line 38 - line 64 column 2, line 61 -column 3, line 20 claims 7-33 ---	11-15
X	DE 199 06 450 C (FRAUNHOFER GES FORSCHUNG) 17 August 2000 (2000-08-17) column 4, line 2 -column 5, line 1 column 9, line 42 - line 46 figure 1 ---	11-15
Y	WO 99 03246 A (LUCENT TECHNOLOGIES INC) 21 January 1999 (1999-01-21) page 6, line 28 -page 7, line 27 figure 2 -----	10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 01/05232

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5805700 A	08-09-1998	NONE	
WO 0060846 A	12-10-2000	US 6415031 B1	02-07-2002
		AU 4330400 A	23-10-2000
		GB 2363278 A	12-12-2001
		WO 0060846 A2	12-10-2000
US 6021199 A	01-02-2000	JP 10145773 A	29-05-1998
		US 6314188 B1	06-11-2001
DE 19906450 C	17-08-2000	DE 19906450 C1	17-08-2000
		AT 219311 T	15-06-2002
		DE 59901773 D1	18-07-2002
		WO 0049763 A1	24-08-2000
		EP 1133849 A1	19-09-2001
WO 9903246 A	21-01-1999	WO 9903246 A2	21-01-1999